How to know if a database should be trusted

⚠ **This page has been made public for vendors**

Question

Fortify has flagged data read from my database as potentially tainted. I trust my database. How can I know that it is trusted?

Answer

Fortify views all data that comes from outside an application as a potential vector for an attack. It therefore marks all data coming into an application as potentially tainted and requires the data to be validated before it is used. This includes data coming in from an application's database.

Best practice is that all data should be validated close to where it is used, including data that is read from a trusted database. This best practice helps ensure all data is validated and that it is validated correctly for how it will be used.

However, the Software Assurance Team recognizes that this is not always feasible for all applications.

To show that a database can be trusted the following criteria is required:

- The developer will need to provide documentation that attests that the database is configured and operated securely according to VA hosting facility policy
- No SQL injection vulnerabilities (**including no findings categorized as Medium or Low by Fortify**) may be present in your application
- All data inserted into the database must be validated appropriately before it is inserted (see below for further information on this)

Validations of the data inserted into the database must be appropriate for how the data is used. If a string retrieved from the database is placed in a web page, it must be validated against cross-site scripting before it is sent to the web page. Any data that is read from a web page must be validated for SQL Injection prior to inserting it into the database. Some developers choose to validate the data for cross site scripting before it is placed in the database, however, since best practice is to validate the data close to where it is used, it's usually preferable to validate the data for cross site scripting just before sending it to the web page. The audit comments must include pointers to all places in the code where that data is put in the database and where it is validated so the reviewer can confirm the correct validations are in place.

Additional information

The following are examples of additional criteria that are recommended:

- No other application may have access to tables or views accessed by the application
- Table, row, and/or column-based access controls are in place to limit access to the database application data
- Connection strings used to connect to the database are encrypted or access is restricted to database connections by the production hosting facility according to VA policy
- If the database is not local, connections to the database are encrypted or sensitive data sent across connections is first encrypted by the application

References

- VA Secure Code Review SOP

Request code review tools, validations, and support HERE.